

## MEMORANDUM

To: Sen. Claire Ayer, Chair, Senate Committee on Health and Welfare  
Sen. Jane Kitchel, Chair, Senate Committee on Appropriations  
Rep. Martha Health, Chair, House Committee on Appropriations  
Rep. Michael Fisher, Chair, House Committee on Health Care  
Rep. Ann Pugh, Chair, House Committee on Human Services

From: Mark Larson, Commissioner

Cc: Doug Racine, Secretary, Agency of Human Services  
Lindsey Tucker, Director, VHC; Deputy Commissioner, DVHA

Date: February 11, 2013

Re: VHC Privacy Incidents since December 16, 2013

---

This memo is to notify you of all Vermont Health Connect privacy incidents which Vermont Health Connect (VHC) has reported to the Centers for Medicare & Medicaid Services (CMS) since December 16<sup>th</sup>, 2013.

- On December 22, 2013, a VHC member reported to VHC that they received another member's insurance confirmation notice included in the same envelope as their premium invoice which they received in the mail on December 21, 2013. The incident was the result of a VHC worker inadvertently including a copy of another VHC member's notice in the same envelope. The first VHC member contacted VHC on December 17, 2013 indicating that they could not view their invoice online and a VHC worker indicated they would mail the invoice and in doing so erroneously prepared the mailing with the other member's notice attached. The errant notice included VHC member name address, plan selection, premium credit, and invoice amount. VHC is contacted both members about the error, confirming destruction of the errant notice, and sent both members letters alerting each of the error. VHC also reviewed training protocols with employees to ensure accuracy of member mailings.
- On January 3, 2014, a VHC Broker reported to VHC that they were able to see the account of a VHC member with the same name as their client, but the information was not the information that they entered for their client. On January 2, 2014, prior to realizing the information associated with their client was incorrect, the broker emailed a copy of the other member's premium invoice to their client. Upon investigation, VHC determined that the incident was the result of a health access eligibility unit worker inadvertently withdrawing the original member's account and entering a new account from a paper application from another applicant with the same name and did not disassociate the new account with the original broker account. There were 2 separate disclosures that occurred; the first disclosure occurred when the VHC Broker was able to view the account profile and premium invoice of the other member which included 2 household member names, address, phone number, insurance eligibility, and premium amount;

the second disclosure occurred when the broker inadvertently sent the wrong premium invoice to their client which included 2 household member names, insurance eligibility, and premium amount. No Federal tax information or social security numbers were reported to have been disclosed. The problem was determined to be isolated, was remedied, and the incident did not appear to affect any other VHC members. VHC has contacted the broker and both members about the error, confirmed destruction of the errant invoice, and sent both members letters informing each of the errors. VHC is also reviewing training protocols with the health access eligibility unit to assure that proper procedures are being followed when validating account identity in the database where other accounts with the same user name exist.

- On January 8, 2014, a VHC Member reported to the VHC customer call center that when they logged into their portal account to see if their payment was received they saw a scanned image of a check from another member with the same name. Upon investigation, VHC determined that the incident was the result of its payment processing contractor Benaissance inadvertently assigning the payment and a scan of a check to a VHC account with the same member name. The scan contained a copy of the cancelled check with the member's name and address, VHC account number written on the check, and checking account number and bank routing number. No Federal tax information or social security numbers were reported to have been disclosed. VHC has contacted both members about the error and has sent both members letters informing each of the error. VHC's contractor is working to identifying where the error occurred in its optical and manual check payment processing for validating account identity in the database where other accounts with the same user name exist. To minimize future potential breaches, VHC is tuning off member access to check images on the portal. VHC has reported the incident to the VT AG's office per 9 VSA § 2435.
- On January 8, 2014, a VHC Member reported to the VHC customer call center that when they logged into their portal account to see if their payment was received they saw a scanned image of a check from another member with the same last name. Upon investigation, VHC determined that the incident was the result of its payment processing contractor Benaissance inadvertently assigning the payment and a scan of a cancelled check to a VHC account with a similar member name. The scan contained a copy of the check containing member's name and address, phone number, and checking account number and bank routing number. No Federal tax information or social security numbers were reported to have been disclosed. VHC has contacted both members about the error and has sent both members letters informing each of the error. VHC's contractor is working to identifying where the error occurred in its optical and manual check payment processing for validating account identity in the database where other accounts with the same user name exist. To minimize future potential breaches, VHC is tuning off member access to check images on the portal. VHC has reported the incident to the VT AG's office per 9 VSA § 2435.
- On January 11, 2014, a VHC Member reported to the VHC customer call center that when they logged into their portal account to see if their payment was received they saw a scanned image of a check from another member. Upon investigation, VHC determined that the incident was the result of incorrect information being sent by a VHC staff member to its payment processing contractor. VHC in trying to resolve a non-processed payment inadvertently provided its contractor the improper account information to assign a payment and the scanned image of a check. The scan contained a copy of the check payment for another account which contained a business name, address, checking account number, and bank routing number. No Federal tax information or social security numbers were reported to have been disclosed. To minimize future potential breaches, VHC is tuning off member access to check images on the portal. VHC has contacted both members about the error and has sent both members letters informing each of the error. VHC has reported the incident to the VT AG's office per 9 VSA § 2435.
- On January 13, 2014, a VHC Member reported to the VHC member call center that her Green Mountain Care card (her Medicaid member card) from her ex-boyfriend. Her card had been mailed to the wrong address and her ex-boyfriend delivered it to her. The address where her card was mailed is consistent with

the address that she lived at 2 years ago. At that time, she started an application for coverage through Green Mountain Care but her application was never completed. She had no active coverage prior to her VHC enrollment. VHC has determined that the incident was a result of an error in the data reconciliation between the State's existing eligibility system, ACCESS, and the VHC data system. Currently, not all self-attestation information from VHC consumers is being loaded into the current ACCESS eligibility database. Questionable data from VHC cannot overwrite ACCESS until it can be properly validated from an external source or through the Federal Data Hub. In this case, this resulted in the address from the VHC user's older application within ACCESS being used instead of the current address provided in the current VHC application. Work is under way to address the programming for validating data in VHC and the data sent from VHC to ACCESS. Until such time as programming is complete, VHC is identifying and reaching out to each questionable case to validate consumer data. VHC has contacted both members about the error and has sent both members letters informing each of the error.

- On January 24, 2014, a VHC Navigator reported to VHC that when they logged into their navigator portal account to view one of their client accounts they could see a scanned image of a check from another member. The Navigator worked with the consumer whose account was the accidental recipient of the scanned check. The Navigator did not work with the consumer who was the sender of the check and had inadvertent access to their scanned check information. The check was only viewable by the navigator as their client does not have a portal account. Upon investigation, VHC determined that the incident was the result of its payment processing contractor inadvertently assigning the payment and a scan of a cancelled check to the incorrect VHC account. The scan contained a copy of the check containing member's name and address, phone number, and checking account number and bank routing number. No Federal tax information or social security numbers were reported to have been disclosed.

To minimize future potential breaches, VHC is turning off member access to check images on the portal. VHC has contacted both the member and the navigator about the error and has sent both letters informing each of the error. VHC has reported the incident to the VT AG's office per 9 VSA § 2435.

VHC has followed its privacy protocols in responding to each of these incidents. VHC has reported each incident to the Centers for Medicare & Medicaid Services, has communicated with all members involved by phone and mail, and where indicated has issued reports to the Vermont Attorney General's Office per state privacy laws. VHC is also making every effort to assure that operations and manual processes are sufficiently detailed and VHC workers are adequately trained and is taking appropriate precautions to avoid future errors.

Based our analysis, these incidents did not include any breach of security or reveal any technology issues that require mitigation.

If you should have any questions please do not hesitate to contact me.